

61. A method according to Claim 60, in which each part is subjected to the digital signature of the said buyer's document carrier which effects the splitting.

REMARKS

With regard to independent claim 25, this claim differs from claim 25 in the parent application in that it states that the secret key of the public-secret key pair is generated **within on the document carrier**. The Rosen patent 5,557,518 cited in the parent application against the original claim 25 does not disclose generation of the secret key on the document carrier. In Rosen, the "MTA" encrypts the "electronic object" and then transfers the electronic object to the customer. Neither the MTA, not the customer, generates the secret key and the MTA does not store the secret key or any derived version thereof. Furthermore, the secret key does not identify the document carrier identifier. In Rosen, a Trusted Agent is required to identify the customer. In the present claim 25, the document carrier is self identifying and unique. The present claim 25 is therefore clearly novel over Rosen.

In addition, claim 25 is inventive over Rosen as there is no teaching from Rosen of the removal of the Trusted Agent. In fact, in order to achieve anonymous payment in Rosen, more than one third party must be involved. The skilled artisan would not read Rosen with a view to removing the Trusted Agent, which is taught as an essential feature, without which Rosen would not work. Rosen also teaches that generation **does not and cannot** occur in the customer money module.

Furthermore, the structural differences between the present claim 25 and Rosen, which provide novelty and inventiveness for the creation of an END, also ensure that the use of the present invention differs from the intended use of Rosen. The intended use of the END created in claim 25, results in a **manipulative difference** in its use, as compared with the prior art, as outlined below.

With regard to independent claims 26 and 37, these claims now state that, as well as mutual recognition being established between respective document carriers, mutual verification, **between** the seller and the buyer, is also established using one or more pre-determined protocols.

The prior art cited in the parent application against these claims, namely Rosen (5,557,518), Pitroda (5,590,038) and Abraham et al. (5,148,481) all require the use of a trusted third party during negotiation. This can be seen in Rosen in Figures 1 and 3 at least and in column 7, lines 56 to 61; column 9, lines 5 to 43; column 17, lines 54 to 60; column 18, lines 40 to 42 and 60 to 65; column 19, lines 13 to 31; column 23, lines 9 to 51, in particular points 1 and 2 of the summary.

Pitroda discloses the requirement of a Trusted Agent to verify in the abstract "after proper verification with the main computer of the service provider...". In addition, Pitroda makes no teaching of the direct contact between two ENDS and the mutual verification before transfer of such an END. Therefore, the skilled artisan could not, starting with Rosen, take Pitroda and combine the two so as to arrive at the present invention. The mutual verification is therefore novel and inventive over the combination of Rosen and Pitroda.

Abraham teaches user verification and user authorization with a trusted third party, but does **not** disclose the mutual verification between two document carriers for the transfer of an END. In addition, Abraham discloses the step of "checking whether the current user is authorized to execute the particular quest to command. A user's authority is defined by the contents of a related user profile in the table of user profiles". Therefore, the table of user profiles, which is stored on the network, is a trusted third party between the user and resource required. There is no teaching in Abraham of mutual verification between two document carriers; in fact, Abraham specifically teaches that the verification may occur at any one of a number of nodes within the network. This is completely contrary to the aim of the present invention, which is to identify and verify the two document carriers involved in the negotiation without any doubt. Therefore, starting with Rosen, combining Abraham would not give results according to the current invention and gives no teaching whatsoever of such. The Abraham reference in fact teaches away from the current invention so that the skilled artisan would not even think to combine these two references. Therefore, the present invention is novel and inventive over the combination of these prior art documents.

The whole purpose of the present invention is that only the negotiating parties (the buyer and seller) need participate in the protocol, without the involvement of a Trusted Agent or any other third party, i.e. to describe a 2-party protocol rather than a 3-party protocol. None of the prior art identifies or addresses such a 2-party protocol; all require the use of a Trusted Third Party.

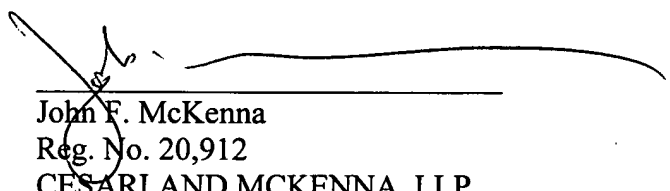
In addition to this, an (electronic) negotiable document is something of value (like a bank note) that can be handed over from the current owner to a new chosen owner in payment many, many times and each time it is transferred, it gives good title to the holder. Rosen and the other prior art do not even in a single sentence, nor in all the examples, give a single mention of this chain of transfer of title for the very reason that their items (tickets) etc. are **not** negotiable instruments.

With regard to Claim 60, this claim differs from claim 60 in the parent application on that it recites that when the END is split, the sum of the values of the parts so created is conserved as the same as the value of the original END. This differentiates between the present invention and Halter et al. patent 5,319,705 cited agent claim 60 in the parent application in that in Halter et al., there is no restriction on sending copies of each part to more than one buyer, each of which is equally valid. It is therefore a money/source generating operation, not a money transfer operation. This distinction therefore introduces novel subject matter into the claim. Additionally, the whole essence of the Halter citation is to allow the multiple copying of the parts created. The teaching is completely against the transfer and conservation of value. In addition, there is no teaching therein of how to achieve such conservation. Therefore, there is two-fold level of inventiveness in this claim in that the prior art does not teach the advantage of making such conservation and it makes no attempt to teach how to address this unidentified problem. Therefore, Claim 60 is clearly patentable over Halter et al. and the other prior art in the present application.

The dependent claims are patentable, inter alia, due to their dependence on one or another of the independent claims. For the foregoing reasons, claims 25 to 61 should be allowed.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,



John F. McKenna
Reg. No. 20,912
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500